

On the Optimal Pre-Computation of Window τ NAF for Koblitz Curves

William R. Trost ^{*} and Guangwu Xu [†]

Abstract

Koblitz curves have been a nice subject of consideration for both theoretical and practical interests. The window τ -adic algorithm of Solinas (window τ NAF) is the most powerful method for computing point multiplication for Koblitz curves. Pre-computation plays an important role in improving the performance of point multiplication. In this paper, the concept of optimal pre-computation for window τ NAF is formulated. In this setting, an optimal pre-computation has some mathematically natural and clean forms, and requires $2^{w-2} - 1$ point additions and two evaluations of the Frobenius map τ , where w is the window width. One of the main results of this paper is to construct an optimal pre-computation scheme for each window width w from 4 to 15 (more than practical needs). These pre-computations can be easily incorporated into implementations of window τ NAF. The ideas in the paper can also be used to construct other suitable pre-computations. This paper also includes a discussion of coefficient sets for window τ NAF and the divisibility by powers of τ through different approaches.

Keywords: Elliptic curve cryptography, window τ -non adjacent form, pre-computation

1 Introduction

One of the most important families of elliptic curves in elliptic curve cryptography (ECC) is the Koblitz curves [10]. A Koblitz curve over \mathbb{F}_{2^m} is defined by

$$E_a : y^2 + xy = x^3 + ax^2 + 1,$$

^{*}Department of EE & CS, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA; e-mail: wrtrost@uwm.edu.

[†]Department of EE & CS, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA; e-mail: gxu4uwm@uwm.edu. Research supported in part by the National 973 Project of China (No. 2013CB834205).

where the parameter a is from $\{0, 1\}$. On E_a/\mathbb{F}_{2^m} , the *Frobenius map* is defined as: for point (x, y) that is different from the point at infinity

$$\tau(x, y) = (x^2, y^2),$$

and for the point at infinity \mathcal{O} , $\tau(\mathcal{O}) = \mathcal{O}$.

Let $\mu = (-1)^{1-a}$. Since $\tau^2(P) + 2P = \mu\tau(P)$ for all $P \in E_a(\mathbb{F}_{2^m})$, τ can be interpreted as a complex number defined by $\tau^2 - \mu\tau + 2 = 0$. One can choose

$$\tau = \frac{\mu + \sqrt{-7}}{2}.$$

Therefore the Euclidean domain $\mathbb{Z}[\tau] = \mathbb{Z} + \mathbb{Z}\tau$ can be identified as a set of automorphisms of E_a in the sense that

$$(g + h\tau)P = gP + h\tau(P).$$

for every $P \in E_a(\mathbb{F}_{2^m})$.

In ECC, one considers the situation where $|E_a(\mathbb{F}_{2^m})|$ is *very nearly prime*, that is, $|E_a(\mathbb{F}_{2^m})| = |E_a(\mathbb{F}_2)| \cdot p$ for some prime $p > 2$. The *main subgroup* M of $E_a(\mathbb{F}_{2^m})$ is the subgroup of order p . For $\delta = \frac{\tau^m - 1}{\tau - 1}$, we have the norm $N_a(\delta) = p^1$ and $\delta(P) = \mathcal{O}$ for $P \in M$. The latter yields a useful fact which asserts that for elements ρ and γ in $\mathbb{Z}[\tau]$, if $\rho \equiv \gamma \pmod{\delta}$, then for every $P \in M$,

$$\rho P = \gamma P. \tag{1.1}$$

The Frobenius map τ is an inexpensive operation as squaring in \mathbb{F}_{2^m} can be done efficiently. Based on this, Koblitz [10] proposed a method of computing the point multiplication nP by representing $n = \sum_{i=0}^k c_i \tau^i$ with $c_i \in \{0, 1\}$ and evaluating $\sum_{i=0}^k c_i \tau^i(P)$.

In [13], Solinas developed a width- w window τ -adic method for the efficient computation of nP . The procedure can be briefly described as

1. **Reduction.** Find some suitable $\rho = r_1 + r_2\tau \in \mathbb{Z}[\tau]$ with $|r_1|, |r_2|$ being roughly \sqrt{n} , such that

$$\rho \equiv n \pmod{\delta}.$$

Then by (1.1), computing nP is equivalent to computing ρP .

2. **Window τ -NAF.** Fix a positive integer w . Denote the *coefficient set*

$$\mathcal{C}_{min} = \{c_1, c_3, \dots, c_{2^{w-1}-1}\} \tag{1.2}$$

¹For an element $r_0 + r_1\tau \in \mathbb{Z}[\tau]$, its norm is $N_a(r_0 + r_1\tau) = (r_0 + r_1\tau)(r_0 + r_1\bar{\tau}) = r_0^2 + \mu r_0 r_1 + 2r_1^2$. This norm is dependent of the parameter a .

where c_j is an element with the least norm from the odd congruence class $\bar{j} = \{c \in \mathbb{Z}[\tau] : c \equiv j \pmod{\tau^w}\}$, ($j = 1, 3, \dots, 2^{w-1} - 1$). The width- w τ non-adjacent form of ρ is

$$\rho = \sum_{i=0}^{l-1} \varepsilon_i u_i \tau^i,$$

where $\varepsilon_i \in \{-1, 1\}$ and $u_i \in \mathcal{C}_{min} \cup \{0\}$ with the properties that in any segment $\{u_k, u_{k+1}, \dots, u_{k+w-1}\}$ of length w , there is at most one nonzero u_i . We denote the above expression of ρ by $\tau\text{NAF}_w(n)$.

3. **Pre-Computation:** Compute $Q_j = c_j P$ for each $j = 1, 3, \dots, 2^{w-1} - 1$. Note that $c_1 = 1$, so $Q_1 = P$ needs no calculation.
4. **Computing nP :** Evaluate ρP by Horner's rule, using $\tau\text{NAF}_w(n)$ and precomputed $Q_1, Q_3, \dots, Q_{2^{w-1}}$. Discarding the zero coefficients, the $\tau\text{NAF}_w(n)$ of ρ can be written as

$$\rho = \underbrace{\varepsilon_0 c_{k_0} \tau^{k_0} + \varepsilon_1 c_{k_1} \tau^{k_1}}_{k_1 - k_0 \geq w} + \underbrace{\varepsilon_2 c_{k_2} \tau^{k_2}}_{k_2 - k_1 \geq w} + \dots + \varepsilon_{s-1} c_{k_{s-1}} \tau^{k_{s-1}} + \underbrace{\varepsilon_s c_{k_s} \tau^{k_s}}_{k_s - k_{s-1} \geq w}$$

with $\varepsilon_j \in \{-1, 1\}$ and $c_{k_j} \in \mathcal{C}_{min}$. So $nP = \rho P$ can be computed through

$$nP = \tau^{k_0} (\tau^{k_1 - k_0} (\dots (\tau^{k_s - k_{s-1}} \varepsilon_s Q_{j_{k_s}} + \varepsilon_{s-1} Q_{j_{k_{s-1}}}) + \dots + \varepsilon_1 Q_{j_{k_{i_1}}}) + \varepsilon_0 Q_{j_{k_0}}).$$

As indicated in [13], for practical values of w , pre-computation requires $2^{w-2} - 1$ point additions. The example (Table 1) given in [13] shows how to construct the pre-computation for the case of $w = 5, a = 1$, i.e.,

Table 1: **Pre-computation from [13]**

$Q_3 = \tau^2 P - P$	$Q_5 = \tau^2 P + P$	$Q_7 = -\tau^3 P - P$	$Q_9 = -\tau^3 Q_5 + P$
$Q_{11} = -\tau^2 Q_5 - P$	$Q_{13} = -\tau^2 Q_5 + P$	$Q_{15} = \tau^4 P - P$	

It can be seen that, in addition to $2^{w-2} - 1 = 7$ point additions, 7 evaluations of τ are also needed, i.e., we need to compute $\tau P, \tau^2 P, \tau^3 P, \tau^4 P$ and $\tau Q_5, \tau^2 Q_5, \tau^3 Q_5$.

Some improved pre-computations are discussed in [7] where eight cases (i.e., $3 \leq w \leq 6, a = 0, 1$) of pre-computation schemes are described. For the case of $w = 5, a = 1$, the following pre-computation given in [7] uses 6 evaluations of τ :

Table 2: **Pre-computation from [7]**

$Q_3 = \tau^2 P - P$	$Q_5 = \tau^2 P + P$	$Q_7 = -\tau^3 P - P$	$Q_9 = -\tau^3 Q_5 + P$
$Q_{11} = -\tau^2 Q_5 - P$	$Q_{13} = -\tau^2 Q_5 + P$	$Q_{15} = \tau^2 Q_5 - Q_5$	

Such pre-computation have been used in the discussion of [1].

In [3], Blake, Murty and Xu extended Solinas's method by allowing a general coefficient set of the form

$$\mathcal{C}_{nm} = \{c_1, c_3, \dots, c_{2^{w-1}-1}\} \quad (1.3)$$

where $c_1 = 1$ and c_j is an element from the odd congruence class \bar{j} that satisfies $N(c_j) < 2^w$, for $j = 3, \dots, 2^{w-1} - 1$. It is easy to see that \mathcal{C}_{min} is a special case of \mathcal{C}_{nm} . It has been proved in [3] that the algorithm for computing $\tau\text{NAF}_w(\rho)$ (Algorithm 4 of [13]) is correct for the general coefficient sets. In particular, [3] provided a termination proof of $\tau\text{NAF}_w(\rho)$ for the original setting of \mathcal{C}_{min} . See also [4].

Examples of efficient pre-computation were given in [3]. For the case $w = 5, a = 1$, example 3 of [3] greatly improved that of [13] by requiring only two evaluations of τ . The pre-computation is

Table 3: **Pre-computation from [3]**

$Q_3 = \tau^2 P - P$	$Q_5 = \tau P - P$	$Q_7 = \tau P + P$	$Q_9 = \tau P + Q_3$
$Q_{11} = \tau P + Q_5$	$Q_{13} = \tau P + Q_7$	$Q_{15} = \tau P + Q_9$	

This pre-computation is actually an optimal one (as explained later).

The purpose of this paper is to systematically study pre-computation for window τNAF for Koblitz curves. As we shall see later, for each $w > 2$, a pre-computation requires at least $2^{w-2} - 1$ point additions and two evaluations of τ (except for the simple case of $w = 3$ where one application of τ is sufficient). We shall call a pre-computation that involves $2^{w-2} - 1$ point additions and two evaluations of τ an *optimal pre-computation*. One of the main results of this paper is to show that for each of the cases $4 \leq w \leq 15, a = 0, 1$, an optimal pre-computation exists. These cover all of practical interesting cases².

A computationally efficient criterion for divisibility of an element $g + h\tau \in \mathbb{Z}[\tau]$ by a power of τ is needed in determining a residue modulo τ^w . This is a useful step for

²As indicated in [13], $w > 8$ is no longer practical, due to the fact that the total cost of using window τNAF is roughly $\frac{m}{w+1} + 2^{w-2} - 1$ point additions

forming the coefficient set \mathcal{C}_{nm} for the window τ NAF, hence for the pre-computation. Such criterion was described by Solinas [13] in terms of Lucas sequences. In this paper, we present a different approach by refining the p -adic argument of Blake, Murty and Xu [4]. This also provides an explanation of the divisibility by a power of τ in the ring $\mathbb{Z}[\tau]$ from another view point. The generality of the computational procedure for divisibility is also useful in our construction of optimal pre-computations.

The rest of the paper is organized into three sections. The next section discusses the algebraic setup of pre-computations. Section 3 will be devoted to a detailed formulation and description of optimal pre-computations. The last section is the conclusion.

2 The Coefficient Sets for Window τ NAF

In our discussion in the previous section, for Koblitz curves, the point multiplication nP can be turned into a complex multiplication $(r_1 + r_2\tau)P$ for $r_1, r_2 \in \mathbb{Z}$. Efficiency can be archived by using the window τ NAF of $r_1 + r_2\tau$. In this section, we shall consider the construction of the coefficient sets for window τ NAF. To this end, we need to work with the (algebraic) integer ring $\mathbb{Z}[\tau] = \{g + h\tau : g, h \in \mathbb{Z}\}$.

Given a positive integer w , the coefficient set \mathcal{C}_{nm} for window τ NAF is the key ingredient for the pre-computation. Recall that \mathcal{C}_{nm} is constructed by taking one element from each odd congruence class \bar{j} modulo τ^w whose norm is less than 2^w , for $j = 1, 3, \dots, 2^{w-1} - 1$.

For each $j = 3, \dots, 2^{w-1} - 1$, define

$$R_j = \{g + h\tau : g + h\tau \equiv j \pmod{\tau^w}, N_a(g + h\tau) < 2^w\}.$$

Assume that an explicit coefficient set is

$$\mathcal{C}_{nm} = \{c_1, c_3, \dots, c_{2^{w-1}-1}\}$$

where $c_1 = 1$ and $c_j \in R_j$ for $j = 3, \dots, 2^{w-1} - 1$. We can see that in the setting of [3], the coefficient sets for a window τ NAF (or pre-computations) are quite flexible. There are

$$\prod_{k=1}^{2^{w-2}-1} |R_{2k+1}|$$

choices of \mathcal{C}_{nm} .

In order to determine the set R_j , we need to find suitable $g + h\tau$ such that $\tau^w | g - j + h\tau$. The problem of divisibility by a power of τ was studied in [13]. Using the Lucas sequence, Solinas proved that there is an integer t_w such that

$$\tau^w | g + h\tau \iff 2^w | g + ht_w. \tag{2.1}$$

In [4], a p -adic approximation approach was proposed for the problem of divisibility by a power of a zero of a quadratic polynomial of the form $X^2 + kX + p$ with $|k| < p$. Here we give an intuitive and a computational refinement of the argument for the case $p = 2$ and polynomial $f(X) = X^2 - \mu X + 2$. Using Hensel's lifting algorithm [8, 12], starting from $s_1 = 0$, we can get the n th 2-adic approximation

$$s_n = b_1 2 + b_2 2^2 + \cdots + b_{n-1} 2^{n-1}$$

of the 2-adic zero $\alpha = \sum_{k=1}^{\infty} b_k 2^k$ of $f(X)$ by the following procedure:

Procedure 2.1: The n th 2-adic Approximation

```

s1 ← 0;
for ( i from 1 to n - 1 ) do
    bi ←  $\frac{f(s_i)}{2^i} \mu \pmod{2}$  ; // f(si) is divisible by 2i.
    si+1 ← si + bi 2i;

```

By this procedure, we can easily get:

s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	\cdots
2μ	6μ	6μ	6μ	38μ	38μ	166μ	422μ	\cdots

In general, we can get a positive integer q_n such that

$$s_n = q_n \mu. \tag{2.2}$$

Note that $2|\alpha$ and $2^n|\alpha - s_n$, so we have

$$\alpha^n |g + h\alpha \iff 2^n |g + hs_n.$$

This naturally leads to the following argument

$$\tau^w |g + h\tau \iff 2^w |g + hs_w. \tag{2.3}$$

We will not explain the proof of (2.3) here, as a rigorous proof of the general p -adic case has already been given in [4].

Note that

$$N_a(g + h\tau) = g^2 + \mu gh + 2h^2 = \frac{3g^2}{4} + \left(\frac{g}{2} + \mu h\right)^2 + h^2,$$

so the requirement $N_a(g + h\tau) < 2^w$ forces $|g| \leq \lfloor \frac{2^{\frac{w+2}{2}}}{\sqrt{3}} \rfloor$ and $|h| \leq \lfloor 2^{\frac{w}{2}} \rfloor$. With these, we are able to describe a method for generating R_j ($j = 3, \dots, 2^{w-1} - 1$):

Procedure 2.2: Generation of R_j

```

 $R_j \leftarrow \emptyset;$ 
for (  $h$  from  $-\lfloor 2^{\frac{w}{2}} \rfloor$  to  $\lfloor 2^{\frac{w}{2}} \rfloor$  ) do
  for (  $g$  from  $-\lfloor \frac{2^{\frac{w+2}{2}}}{\sqrt{3}} \rfloor$  to  $\lfloor \frac{2^{\frac{w+2}{2}}}{\sqrt{3}} \rfloor$  ) do
    if (  $(2^w | g - j + h s_w)$  and  $(g^2 + \mu gh + 2h^2 < 2^w)$  )
      append  $(g + h\tau)$  to  $R_j;$ 

```

3 Optimal Pre-computations

Once a coefficient set $\mathcal{C}_{nm} = \{c_1, c_3, \dots, c_{2^{w-1}-1}\}$ is specified, the pre-computation can be performed. Given the base point P , this is the task for computing and storing the $2^{w-2} - 1$ points

$$Q_3 = c_3 P, \quad Q_5 = c_5 P, \quad \dots, \quad Q_{2^{w-1}-1} = c_{2^{w-1}-1} P.$$

For the sake of convenience, in the rest discussion, we set $c_1 = 1$ and $Q_1 = P$. We also remark that the pre-computations for the case of $w = 3$ is very simple and only Q_3 needs to be computed:

Pre-computation for $w = 3$

$a = 0$	$Q_3 = P + \tau(P)$	$a = 1$	$Q_3 = P - \tau(P)$
---------	---------------------	---------	---------------------

So we shall be interested in the cases of $w > 3$ in the rest of the section. Another remark we would like to make is that an efficient pre-computation may be achieved with rearranging the order of $Q_1, Q_3, Q_5, \dots, Q_{2^{w-1}-1}$. In the actual computation, we may need to compute some Q_j before Q_k , even though $j > k$.

Now we begin the setup of optimal pre-computation.

We first observe that there are only two elliptic curve operations involved in the pre-computation, the point addition (include point doubling) and evaluation of τ . As pointed out in [13], for w in the practical range (for w from 3 to 8), each Q_j ($j \geq 3$) can be done by using one point addition operation, plus some evaluations of τ . The cost of the latter is comparatively less.

Next we argue that, in terms of point addition operation, one operation for each Q_j ($j = 3, 5, \dots, 2^{w-1} - 1$) is necessary. If not, suppose that some Q_{j_0} is obtained by only using τ to some previous computed Q_k (this should include $Q_1 = P$). This means that $c_{j_0} = \tau^e c_k$. Note that j_0 is an odd number, so $j_0 \equiv 1 \pmod{\tau}$ (since $2 = \tau(\mu - \tau)$). Therefore

$$\begin{aligned} \tau^e c_k &= c_{j_0} \equiv j_0 \pmod{\tau^w} \\ &\equiv 1 \pmod{\tau}. \end{aligned}$$

This implies that there is a $u \in \mathbb{Z}[\tau]$ such that

$$\tau u = 1.$$

This is absurd as $N_a(\tau u) = N_a(\tau)N_a(u) = 2N_a(u) > 1$. Thus point addition operation must be used in computing Q_j ($j \geq 3$).

Finally, we turn to the other operation, the Frobenius map τ . Concerning the efficiency of using τ in pre-computation, there has not been a clean argument yet. As mentioned earlier, the example in [13] discussed the case $w = 5, a = 1$, and 7 evaluations of τ were needed. An improvement for this case was suggested in [7] with 6 evaluations of τ . The other cases discussed in [7] include $w = 4$ (with 3 evaluations of τ) and $w = 6$ (with 12 evaluations of τ). For the case $w = 5, a = 1$, a more efficient pre-computation scheme was proposed in [3]. This scheme uses only two evaluations of τ , namely $\tau(P)$ and $\tau(\tau(P))$. The interesting fact is that this is the best one can do. In general, we can argue that under the assumption that $4 \leq w \leq 15$, and only one point addition is allowed for each Q_j ($j = 3, 5, \dots, 2^{w-1} - 1$), then we need at least two evaluations of τ to finish the pre-computation. In fact, suppose we have a pre-computation

$$Q_{j_1} = P, \quad Q_{j_3}, \quad Q_{j_5}, \quad \dots, \quad Q_{j_{2^{w-1}-1}}.$$

Since Q_{j_3} is the first term that needs to be computed, it must be of the form of $\varepsilon_1 P + \varepsilon_2 \tau^e(P)$, where $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$ and $e \geq 1$. Assume that we could get the pre-computation done by using only one evaluation of τ , then this evaluation must be $\tau(P)$. So $e = 1$ and for each $k > 3$, we have

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 \tau(P),$$

for some $l < k$ and $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$. In terms of the elements in the coefficient set \mathcal{C}_{nm} , this means that for each $k > 3$, there is an $l < k$ and $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, such that

$$c_{j_k} = \varepsilon_1 c_{j_l} + \varepsilon_2 \tau. \tag{3.1}$$

This has been proved to be impossible by checking all possible sets of \mathcal{C}_{nm} .

Based on these discussions, we define an *optimal pre-computation* for $Q_1, Q_3, Q_5, \dots, Q_{2^{w-1}-1}$ to be a pre-computation satisfying

1. Computation of each of $Q_3, Q_5, \dots, Q_{2^{w-1}-1}$ uses only one point addition;
2. The entire pre-computation uses only two special evaluations of τ , namely $\tau(P)$ and $\tau(\tau(P))$.

We would like to point out that this formulation of optimal pre-computation is mathematically natural and clean. In particular, if an optimal pre-computation for the curve $y^2 + xy = x^3 + 1/\mathbb{F}_{2^m}$ (ie., the parameter $a = 0$) is found, then an optimal pre-computation for the curve $y^2 + xy = x^3 + x^2 + 1/\mathbb{F}_{2^m}$ (ie., the parameter $a = 1$) can be constructed immediately, and vice versa. These are proven in the following proposition.

Proposition 3.1 *Assume that an optimal pre-computation with Q_j 's are computed in the following order*

$$Q_{j_1} = P, \quad Q_{j_3}, \quad Q_{j_5}, \quad \dots, \quad Q_{j_{2^w-1-1}}.$$

Then

1. For each $k \geq 3$, there is an $l < k$ and $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$ such that

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 \tau^e(P), \tag{3.2}$$

with $e = 1$ or 2 .

2. If an optimal pre-computation of the form (3.2) is found for $a = 0$ ($a = 1$), then we have an optimal pre-computation $Q_{j_1} = P, \quad Q_{j_3}, \quad Q_{j_5}, \quad \dots, \quad Q_{j_{2^w-1-1}}$ for $a = 1$ ($a = 0$) with the following form

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 (-1)^e \tau^e(P),$$

Proof.

1. Since Q_{j_k} is formed using one addition, it can be either

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 Q_{j_d},$$

for $l, d < k$, or

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 \tau^e(P),$$

for $l < k$ and $e = 1$ or 2 .

Thus we only need to prove the first case is false. Indeed, as c_{j_l} and c_{j_d} are chosen from odd congruence classes, and both have smaller norms, representing the relation $Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 Q_{j_d}$ as

$$c_{j_k} P = (\varepsilon_1 c_{j_l} + \varepsilon_2 c_{j_d}) P,$$

we get $c_{j_k} = (\varepsilon_1 c_{j_l} + \varepsilon_2 c_{j_d})$. This implies that c_{j_k} is in an even congruence class. However, the coefficients must be from odd classes, so this is a contradiction.

2. Let $a = 0$ and an optimal pre-computation is of the form (3.2). This means that Q_{j_3} must be of the form $\varepsilon_1 P + \varepsilon_2 \tau^e(P)$, and each following Q_{j_k} is obtained by adding $\varepsilon_3 \tau^{e'}(P)$ to some previous one. So Q_{j_k} can be written as

$$Q_{j_k} = \varepsilon P + z_1 \tau(P) + z_2 \tau^2(P), \quad \text{for } \varepsilon \in \{-1, 1\} \text{ and some } z_1, z_2 \in \mathbb{Z}. \tag{3.3}$$

This, together with the fact that $\tau^2 = \mu\tau - 2$, mean that,

$$c_{j_k} = \varepsilon + z_1 \tau + z_2 \tau^2 = (\varepsilon - 2z_2) + (z_1 + \mu z_2) \tau.$$

Since $c_{j_k} \equiv j_k \pmod{\tau^w}$, by (2.3) and (2.2), we have

$$2^w | (\varepsilon - 2z_2 - j_k) + (z_1 + \mu z_2) q_w \mu.$$

Note that in this case, $\mu = (-1)^{1-a} = -1$, so we have

$$2^w | (\varepsilon - 2z_2 - j_k) + (z_2 - z_1) q_w. \quad (3.4)$$

Now consider the case of $a = 1$. In this case, $\mu = (-1)^{1-a} = 1$. So (3.4) can be reorganized as

$$2^w | (\varepsilon - 2z_2 - j_k) + (-z_1 + \mu z_2) q_w \mu.$$

Using (2.3) again, we see that $\tau^w | (\varepsilon - 2z_2 - j_k) + (-z_1 + \mu z_2) \tau$, i.e.,

$$\varepsilon - z_1 \tau + z_2 \tau^2 \equiv j_k \pmod{\tau^w}.$$

Denote $c'_{j_k} = \varepsilon - z_1 \tau + z_2 \tau^2$, since $N_1(c'_{j_k}) = N_0(c_{j_k})$, so

$$\{1, c'_{j_3}, c'_{j_5}, \dots, c'_{j_{2^w-1-1}}\}$$

is a coefficient set of window τ NAF for the case of $a = 1$. For the corresponding pre-computation, we let $Q_{j_k} = c'_{j_k} P = \varepsilon P - z_1 \tau(P) + z_2 \tau^2(P)$. Observe that we only change the sign of the confident of τ in the expression (3.3), so this pre-computation must satisfy

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 (-1)^e \tau^e(P).$$

The proof of constructing an optimal pre-computation for the case $a = 0$, from the case $a = 1$, is analogous.

■

The main result in this section is to show that for w from 4 to 15, there is always an optimal pre-computation for the window τ NAF.

Theorem 3.1 *For each w from 4 to 15, there exists a coefficient \mathcal{C}_{nm} whose corresponding pre-computation can be arranged as*

$$Q_{j_1} = P, \quad Q_{j_3}, \quad Q_{j_5}, \quad \dots, \quad Q_{j_{2^w-1-1}}.$$

such that for each $k > 3$, there is an $l < k$ and $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, one has either

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 \tau(P),$$

or

$$Q_{j_k} = \varepsilon_1 Q_{j_l} + \varepsilon_2 \tau^2(P).$$

The proof of this result is done by simply displaying all of these optimal pre-computations. We remark that these pre-computations can be easily used in the implementation of window τ NAF.

We will list the pre-computations for the cases of $4 \leq w \leq 8$. The cases of $9 \leq w \leq 15$ can be found at <http://www.cs.uwm.edu/faculty/gxu4uwm/OptPreComp> .

By proposition 3.1, we only need to consider the case of $a = 0$. The case of $a = 1$ can be obtained by changing the sign of the coefficient of τ in each Q_j from the case of $a = 0$ (note that the sign of coefficient for τ^2 remains unchanged) .

Table 4: **Pre-Computations for $4 \leq w \leq 8$ and $a = 0$**

w	Pre-computation		
4	$Q_3 = -P + \tau^2 P$	$Q_5 = -P - \tau P$	$Q_7 = P - \tau P$
5	$Q_3 = -P + \tau^2 P$ $Q_9 = Q_3 - \tau P$ $Q_{15} = -Q_{11} + \tau P$	$Q_5 = -P - \tau P$ $Q_{11} = Q_5 - \tau P$	$Q_7 = P - \tau P$ $Q_{13} = Q_7 - \tau P$
6	$Q_{29} = P - \tau^2 P$ $Q_5 = Q_{31} - \tau P$ $Q_{27} = P + \tau P$ $Q_{13} = -Q_{25} - \tau P$ $Q_{19} = -Q_7 + \tau P$	$Q_3 = Q_{29} - \tau P$ $Q_7 = -Q_{31} - \tau P$ $Q_{11} = -Q_{27} - \tau P$ $Q_{15} = -Q_{11} + \tau P$ $Q_{21} = -Q_{17} - \tau P$	$Q_{31} = Q_3 - \tau^2 P$ $Q_9 = -Q_{29} - \tau P$ $Q_{25} = -P + \tau P$ $Q_{17} = -Q_9 + \tau P$ $Q_{23} = -Q_3 + \tau P$
7	$Q_{35} = -P + \tau^2 P$ $Q_5 = -Q_{33} - \tau P$ $Q_{43} = Q_5 - \tau P$ $Q_{41} = Q_3 - \tau P$ $Q_{39} = P - \tau P$ $Q_{37} = -P - \tau P$ $Q_{55} = -Q_{35} + \tau P$ $Q_{19} = Q_{57} + \tau P$ $Q_{25} = -Q_{13} - \tau P$ $Q_{29} = -Q_{61} + \tau P$ $Q_{63} = Q_{25} - \tau P$	$Q_3 = -Q_{35} - \tau P$ $Q_{31} = -Q_5 + \tau^2 P$ $Q_{47} = -Q_{43} + \tau P$ $Q_{49} = -Q_{41} + \tau P$ $Q_{51} = -Q_{39} + \tau P$ $Q_{53} = -Q_{37} + \tau P$ $Q_{17} = Q_{55} + \tau P$ $Q_{21} = -Q_{17} - \tau P$ $Q_{27} = -Q_{11} - \tau P$ $Q_{45} = Q_7 - \tau P$	$Q_{33} = -Q_3 + \tau^2 P$ $Q_7 = -Q_{31} - \tau P$ $Q_9 = Q_{47} + \tau P$ $Q_{11} = Q_{49} + \tau P$ $Q_{13} = Q_{51} + \tau P$ $Q_{15} = Q_{53} + \tau P$ $Q_{57} = -Q_{33} + \tau P$ $Q_{23} = -Q_{15} - \tau P$ $Q_{61} = Q_{23} - \tau P$ $Q_{59} = -Q_{31} + \tau P$
8	$Q_{93} = P - \tau^2 P$ $Q_5 = Q_{95} - \tau P$ $Q_{85} = -Q_5 + \tau P$ $Q_{87} = -Q_3 + \tau P$	$Q_3 = Q_{93} - \tau P$ $Q_{97} = Q_5 - \tau^2 P$ $Q_{81} = -Q_{85} - \tau P$ $Q_{79} = -Q_{87} - \tau P$	$Q_{95} = Q_3 - \tau^2 P$ $Q_7 = Q_{97} - \tau P$ $Q_9 = -Q_{81} + \tau P$ $Q_{11} = -Q_{79} + \tau P$

Continued on next page

Table 4 – Continued from previous page

w	Pre-computation		
	$Q_{89} = -P + \tau P$	$Q_{77} = -Q_{89} - \tau P$	$Q_{13} = -Q_{77} + \tau P$
	$Q_{91} = P + \tau P$	$Q_{75} = -Q_{91} - \tau P$	$Q_{15} = -Q_{75} + \tau P$
	$Q_{73} = -Q_{93} - \tau P$	$Q_{17} = -Q_{73} + \tau P$	$Q_{71} = -Q_{95} - \tau P$
	$Q_{19} = -Q_{71} + \tau P$	$Q_{69} = -Q_{97} - \tau P$	$Q_{21} = -Q_{69} + \tau P$
	$Q_{99} = Q_7 - \tau^2 P$	$Q_{67} = -Q_{99} - \tau P$	$Q_{23} = -Q_{67} + \tau P$
	$Q_{101} = Q_{11} + \tau P$	$Q_{65} = -Q_{101} - \tau P$	$Q_{25} = -Q_{65} + \tau P$
	$Q_{103} = Q_{13} + \tau P$	$Q_{63} = -Q_{101} - \tau P$	$Q_{27} = -Q_{63} + \tau P$
	$Q_{105} = Q_{15} + \tau P$	$Q_{61} = -Q_{105} - \tau P$	$Q_{29} = -Q_{61} + \tau P$
	$Q_{107} = Q_{17} + \tau P$	$Q_{59} = -Q_{107} - \tau P$	$Q_{31} = -Q_{59} + \tau P$
	$Q_{109} = Q_{19} + \tau P$	$Q_{57} = -Q_{109} - \tau P$	$Q_{33} = -Q_{57} + \tau P$
	$Q_{111} = Q_{21} + \tau P$	$Q_{55} = -Q_{111} - \tau P$	$Q_{35} = -Q_{55} + \tau P$
	$Q_{113} = Q_{23} + \tau P$	$Q_{53} = -Q_{113} - \tau P$	$Q_{37} = -Q_{53} + \tau P$
	$Q_{115} = Q_{23} - \tau^2 P$	$Q_{51} = -Q_{115} - \tau P$	$Q_{39} = -Q_{51} + \tau P$
	$Q_{125} = Q_{35} + \tau P$	$Q_{41} = -Q_{125} - \tau P$	$Q_{123} = Q_{33} + \tau P$
	$Q_{43} = -Q_{123} - \tau P$	$Q_{121} = Q_{31} + \tau P$	$Q_{45} = -Q_{121} - \tau P$
	$Q_{119} = Q_{29} + \tau P$	$Q_{47} = -Q_{119} - \tau P$	$Q_{117} = Q_{27} + \tau P$
	$Q_{49} = -Q_{117} - \tau P$	$Q_{83} = -Q_7 + \tau P$	$Q_{127} = Q_{37} + \tau P$

Finally, we list an optimal pre-computation for $w = 6, a = 1$ based on proposition 3.1.

Table 5: Pre-Computations for $w = 6$ and $a = 1$

w	Pre-computation		
6	$Q_{29} = P - \tau^2 P$	$Q_3 = Q_{29} + \tau P$	$Q_{31} = Q_3 - \tau^2 P$
	$Q_5 = Q_{31} + \tau P$	$Q_7 = -Q_{31} + \tau P$	$Q_9 = -Q_{29} + \tau P$
	$Q_{27} = P - \tau P$	$Q_{11} = -Q_{27} + \tau P$	$Q_{25} = -P - \tau P$
	$Q_{13} = -Q_{25} + \tau P$	$Q_{15} = -Q_{11} - \tau P$	$Q_{17} = -Q_9 - \tau P$
	$Q_{19} = -Q_7 - \tau P$	$Q_{21} = -Q_{17} + \tau P$	$Q_{23} = -Q_3 - \tau P$

We would like to conclude this section by the following remark.

Remark 3.1 *We remark that in some situations, only one evaluation of τ is needed in an optimal pre-computation. Suppose we are choosing the point $P = (x_P, y_P)$ on the elliptic curve E_1/F_{2^m} , then in the process of generation or validation, the equation $y_P^2 + x_P y_P = x_P^3 + x_P^2 + 1$ needs to be involved, so we can save x_P^2 and y_P^2 for later use in the stage*

of pre-computation. In this case, as $\tau(P) = (X_P^2, y_P^2)$ is already available, an optimal pre-computation only requires one evaluation of τ , i.e., $\tau^2 P = \tau(\tau(P))$.

4 Conclusion

Koblitz curves are a family of curves with complex multiplication. The complex multiplication fields for curves $E_1 : y^2 + xy = x^3 + x^2 + 1/\mathbb{F}_{2^m}$ and their “twist” $E_0 : y^2 + xy = x^3 + 1/\mathbb{F}_{2^m}$ is $\mathbb{Q}(\sqrt{-7})$. The window τ NAF algorithm of Solinas is a successful example of exploring the rich mathematical content to design an extremely efficient point multiplication method. This paper presents a systematic study of the pre-computation schemes for τ NAF. We define an optimal pre-computation to be a scheme that allows $2^{w-2} - 1$ point additions and two evaluations of τ , for any given window width $w \geq 4$ (the case of $w = 3$ is simple and only one evaluation of τ is needed). This is a mathematically natural setup in that once an optimal pre-computation for E_a is produced, an optimal pre-computation for its twist E_{1-a} can be obtained without any nontrivial computation. We have constructed optimal pre-computations of w from 4 to 15. These pre-computations can be incorporated into implementations of window τ NAF. The ideas in the paper can be used to construct other suitable pre-computations. In this paper, we also give a criterion for the divisibility by powers of τ in terms of 2-adic approximation. This is useful in our discussion of the coefficient sets of window τ NAF and optimal pre-computation, it might also be of some independent interest.

References

- [1] D. Aranha, A. Faz-Hernández, J. López, Fr. Rodríguez-Henríquez, Faster implementation of scalar multiplication on Koblitz curves, *LatinCryt 2012*, LNCS **7533**, 177-193.
- [2] I. F. Blake, V. K. Murty and G. Xu, Efficient algorithms for Koblitz curves over fields of characteristic three, *Journal of Discrete Algorithms*, 3(2005)113-124.
- [3] I. Blake, K. Murty and G. Xu, A note on window τ -NAF algorithm, *Information Processing Letters*, 95(2005), no. 5, 496-502.
- [4] I. F. Blake, V. K. Murty and G. Xu, Nonadjacent radix- τ expansions of integers in Euclidean imaginary quadratic number fields, *Canadian Journal of Mathematics*, 60(2008), 1267-1282.
- [5] I. F. Blake, G. Seroussi and N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

- [6] I. F. Blake, G. Seroussi and N. Smart, *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.
- [7] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, 2004.
- [8] N. Koblitz, *p*-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer, 1996.
- [9] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48** (1987) 203-209.
- [10] N. Koblitz, CM-curves with good cryptographic properties, *Advances in Cryptology-CRYPTO '91*, LNCS **576**, 1992, 279-287.
- [11] N. Koblitz, An elliptic curves implementation of the finite field digital signature algorithm, *Advances in Cryptology-CRYPTO '98*, LNCS **1462**, 327-337.
- [12] M. R. Murty, *Introduction to p-adic Analytic Number Theory*, Amer Math. Soc., 2002.
- [13] J. Solinas, Efficient arithmetic on Koblitz curves, *Designs, Codes and Cryptography*, **19** (2000), 195-249.
- [14] W. Trost, Pre-computation in Width- w τ -adic NAF Implementations on Koblitz Curves, *MS Thesis, University of Wisconsin-Milwaukee, May 2014*.